Office of the Information and Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Loblaw Companies Limited (Organization)
Decision number (file number)	P2015-ND-74 (File #P2913)
Date notice received by OIPC	November 17, 2014
Date Organization last provided information	February 6, 2015
Date of decision	November 9, 2015
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is federally incorporated, and qualifies as an "organization" as defined in section 1(1)(i)(iv) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • telephone number, • email address, • points earned, redeemed or used in the last 12 months, • security question, • security answer, • primary sign in email, • secondary email, • member card numbers, • partial debit and credit card numbers (last four digits). This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.

DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• As a result of an error implementing a system change affecting website performance, user information became available to other users who were logged into the system. Specifically, customers attempting to view their own accounts were inadvertently able to view part or all of another member's account information. • A total of 2705 individual members accessed the website during the relevant time period. Of these, the Organization determined a maximum of 1166 individuals could have potentially viewed another member's personal information.
Affected individuals	A total of 1166 individuals in Canada were affected, including 194 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Implemented additional technical validation processes. • Provided additional staff training. • Complete review of tool used for website.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail (or email if no physical address was on file) and telephone in November 2014.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported the information at issue is of low to moderate sensitivity, and could be used to cause the harm of identity theft. I agree with the Organization. The personal information involved could be used to cause identity theft and fraud. It also includes email addresses, which could be used for phishing purposes. In my view, these are significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization submitted that, given the nature of the information at issue, the risk of harm is low. In addition, due to the technical system design, no one member's personal information would have been exposed for more than one hour. In my view, the risk of harm is decreased because the incident resulted from human error, rather than malicious intent, and because no one member's information was exposed for more than one hour. However, the risk of harm is increased because of the number of individual exposures (over 1100).

DECISION UNDER SECTION 37.1(1) OF PIPA
Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals. The personal information involved could be used to cause the significant harms of phishing, identity theft, and fraud. Although the incident resulted from human error, and the information was exposed for a limited time, the risk of harm is increased because of the number of individual exposures (over 1100). I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified individuals affected by the incident in accordance with section 19.1 of the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner